

FINITE MODULES OVER  $\mathbb{Z}[t, t^{-1}]$ 

XIANG-DONG HOU

ABSTRACT. Let  $\Lambda = \mathbb{Z}[t, t^{-1}]$  be the ring of Laurent polynomials over  $\mathbb{Z}$ . We classify all  $\Lambda$ -modules  $M$  with  $|M| = p^n$ , where  $p$  is a prime and  $n \leq 4$ . Consequently, we have a classification of Alexander quandles of order  $p^n$  for  $n \leq 4$ .

## 1. INTRODUCTION

Let  $\Lambda = \mathbb{Z}[t, t^{-1}]$  be the ring of Laurent polynomials over  $\mathbb{Z}$ , which is also the group ring over  $\mathbb{Z}$  of the infinite cyclic group. Each  $\Lambda$ -module is uniquely determined by a pair  $(M, \alpha)$ , where  $M$  is an abelian group and  $\alpha \in \text{Aut}_{\mathbb{Z}}(M)$ . The resulting  $\Lambda$ -module, denoted by  $M_{\alpha}$ , is  $M$  with a scalar multiplication defined by  $tx = \alpha(x)$ ,  $x \in M$ . If two  $\Lambda$ -modules  $M_{\alpha}$  and  $N_{\beta}$  are isomorphic, where  $\alpha \in \text{Aut}_{\mathbb{Z}}(M)$  and  $\beta \in \text{Aut}_{\mathbb{Z}}(N)$ , then  $M \cong N$  as abelian groups. Moreover, for  $\alpha, \beta \in \text{Aut}_{\mathbb{Z}}(M)$ ,  $M_{\alpha} \cong M_{\beta}$  if and only if  $\alpha$  and  $\beta$  are conjugate in  $\text{Aut}_{\mathbb{Z}}(M)$ . Thus, to classify  $\Lambda$ -modules with an underlying abelian group  $M$  is to determine the conjugacy classes of  $\text{Aut}_{\mathbb{Z}}(M)$ .

Our interest in finite  $\Lambda$ -modules comes from topology. In knot theory, a *quandle* is defined to be a set of  $Q$  equipped with a binary operation  $*$  such that for all  $x, y, z \in Q$ ,

- (i)  $x * x = x$ ,
- (ii)  $(\ ) * y$  is a permutation of  $Q$ ,
- (iii)  $(x * y) * z = (x * z) * (y * z)$ .

Finite quandles are used to color knots; the number of colorings of a knot  $K$  by a finite quandle  $Q$  is an invariant of  $K$  which allows us to distinguish inequivalent knots effectively [1, 2].

An *Alexander quandle* is a  $\Lambda$ -module  $M$  with a quandle operation defined by  $x * y = tx + (1 - t)y$ ,  $x, y \in M$ . The following theorem is of fundamental importance.

**Theorem 1.1** ([8]). *Two finite Alexander quandles  $M$  and  $N$  are isomorphic if and only if  $|M| = |N|$  and the  $\Lambda$ -modules  $(1 - t)M$  and  $(1 - t)N$  are isomorphic.*

Therefore, the classification of finite Alexander quandles is essentially the classification of finite  $\Lambda$ -modules.

The classification of finite  $\Lambda$ -modules can be reduced to that of  $\Lambda$ -modules of order  $p^n$ , where  $p$  is a prime; see section 2. The same is true for the classification of finite Alexander quandles; see section 4. Finite Alexander quandles have been classified for orders up to 15 in [8] and for order 16 in [6, 7]. Also known is the classification of connected Alexander quandles of order  $p^2$  [3, 8]. (A finite Alexander quandle is called *connected* if  $1 - t \in \text{Aut}_{\mathbb{Z}}(M)$ .) The purpose of the present paper

2000 *Mathematics Subject Classification.* 16S34, 20K01, 57M27.

*Key words and phrases.* Alexander quandle, finite module, knot, group ring.

is to classify all  $\Lambda$ -modules and Alexander quandles of order  $p^n$ ,  $n \leq 4$ . The details of the classification are given in Table 1 in the appendix. For a snapshot, there are  $5p^4 - 2p^3 - 2p - 1$  nonisomorphic  $\Lambda$ -modules of order  $p^4$  and there are  $5p^4 - 6p^3 + p^2 - 6p - 1$  nonisomorphic Alexander quandles of order  $p^4$ .

In section 2, we show that every finite  $\Lambda$ -module has a unique decomposition where each direct summand  $M$  has the following properties:

- (i)  $|M| = p^n$  for some prime  $p$  and integer  $n > 0$ .
- (ii) When treating  $t$  as an element of  $\text{End}_{\mathbb{Z}_p}(M/pM)$ , the minimal polynomial of  $t$  is a power of some irreducible  $f \in \mathbb{Z}_p[X]$ .

In section 3, we classify such  $\Lambda$ -modules  $M$  of order  $p^n$  with  $n \leq 4$ . In section 4, we derive the classification of Alexander quandles of order  $p^n$ ,  $n \leq 4$ , from the results of section 3. For this purpose, we prove the following fact which is of interest in its own right: Given a finite  $\Lambda$ -module  $N$  and an integer  $l > 0$ , a necessary and sufficient condition for the existence of a  $\Lambda$ -module  $M \supset N$  such that  $(1-t)M = N$  and  $|M/N| = l$  is  $|N/(1-t)N| \mid l$ .

In our notation, the letter  $t$  is reserved for the element  $t \in \Lambda = \mathbb{Z}[t, t^{-1}]$ . The group of units of a ring  $R$  is denoted by  $R^\times$ ; the set of all  $m \times n$  matrices over  $R$  is denoted by  $M_{m \times n}(R)$ .

## 2. DECOMPOSITION OF FINITE $\Lambda$ -MODULES

Let  $M$  be a finite  $\Lambda$ -module. For each prime  $p$ , let

$$M_p = \{x \in M : p^n x = 0 \text{ for some } n \geq 0\}.$$

It is quite obvious that

$$(2.1) \quad M = \bigoplus_p M_p.$$

Moreover, two finite  $\Lambda$ -modules  $M$  and  $N$  are isomorphic if and only if  $M_p \cong N_p$  for all primes  $p$ .

**Theorem 2.1.** *Let  $M$  be a finite  $\Lambda$ -module with  $|M| = p^n$ . For each irreducible  $f \in \mathbb{Z}_p[X]$ , let  $\bar{f} \in \mathbb{Z}[X]$  be a lift of  $f$  and define*

$$(2.2) \quad M_f = \{x \in M : \bar{f}(t)^m x = 0 \text{ for some } m \geq 0\}.$$

*Then*

$$(2.3) \quad M = \bigoplus_f M_f,$$

*where  $f$  runs over all irreducible polynomials in  $\mathbb{Z}_p[X]$ . Moreover, if  $N$  is another finite  $\Lambda$ -module whose order is a power of  $p$ , then  $M \cong N$  if and only if  $M_f \cong N_f$  for all irreducible  $f \in \mathbb{Z}_p[X]$ .*

**Note.**  $M_f$  depends only on  $f$  but not on  $\bar{f}$ . Also,  $M_f = 0$  unless  $f$  divides the minimal polynomial of  $t$  (viewed as an element of  $\text{End}_{\mathbb{Z}_p}(M/pM)$ ).

*Proof of Theorem 2.1.*  $1^\circ$  Let the minimal polynomial of  $t$  ( $\in \text{End}_{\mathbb{Z}_p}(M/pM)$ ) be  $f_1^{e_1} \cdots f_k^{e_k}$ , where  $f_1, \dots, f_k \in \mathbb{Z}_p[X]$  are distinct irreducibles and  $e_1, \dots, e_k$  are positive integers. We claim that

$$(2.4) \quad M = \bigoplus_{1 \leq i \leq k} M_{f_i}.$$

We first show that  $\sum_{1 \leq i \leq k} M_{f_i}$  is a direct sum. Assume that  $x \in M_{f_i} \cap (\sum_{1 \leq j \leq k, j \neq i} M_{f_j})$ . Then there exists  $m > 0$  such that  $\overline{f_i}(t)^m x = 0$  and  $(\prod_{1 \leq j \leq k, j \neq i} \overline{f_j}(t))^m x = 0$ . Since  $\gcd(f_i, \prod_{1 \leq j \leq k, j \neq i} f_j) = 1$ , there exist  $u, v \in \mathbb{Z}_p[X]$  such that

$$uf_i^m + v\left(\prod_{\substack{1 \leq j \leq k \\ j \neq i}} f_j\right)^m = 1.$$

Let  $\overline{u}, \overline{v} \in \mathbb{Z}[X]$  be arbitrary lifts of  $u, v$ , respectively. Then

$$\overline{u}\overline{f_i}^m + \overline{v}\left(\prod_{\substack{1 \leq j \leq k \\ j \neq i}} \overline{f_j}\right)^m \equiv 1 \pmod{p}.$$

Therefore

$$\overline{u}(t)\overline{f_i}(t)^m + \overline{v}(t)\left(\prod_{\substack{1 \leq j \leq k \\ j \neq i}} \overline{f_j}(t)\right)^m \in \text{Aut}_{\mathbb{Z}}(M).$$

Since

$$\left[\overline{u}(t)\overline{f_i}(t)^m + \overline{v}(t)\left(\prod_{\substack{1 \leq j \leq k \\ j \neq i}} \overline{f_j}(t)\right)^m\right]x = 0,$$

we have  $x = 0$ .

Now we prove that  $M = \sum_{1 \leq i \leq k} M_{f_i}$ . There exist  $u_1, \dots, u_k \in \mathbb{Z}_p[X]$  such that

$$\sum_{1 \leq i \leq k} u_i \left(\prod_{\substack{1 \leq j \leq k \\ j \neq i}} f_j^{e_j}\right)^n = 1.$$

Let  $\overline{u_i} \in \mathbb{Z}[X]$  be a lift of  $u_i$  and let  $F_i = \prod_{1 \leq j \leq k, j \neq i} \overline{f_j}^{e_j}$ . Then

$$\sum_{1 \leq i \leq k} \overline{u_i} F_i^n \equiv 1 \pmod{p}.$$

Thus  $\sum_{1 \leq i \leq k} \overline{u_i}(t) F_i(t)^n \in \text{Aut}_{\mathbb{Z}}(M)$ . It follows that

$$(2.5) \quad M = \sum_{1 \leq i \leq k} F_i(t)^n M.$$

Since  $(\prod_{1 \leq j \leq k} \overline{f_j}(t)^{e_j})M \subset pM$ , we have

$$\overline{f_i}(t)^{e_i n} F_i(t)^n M = \left(\prod_{1 \leq j \leq k} \overline{f_j}(t)^{e_j}\right)^n M \subset p^n M = 0.$$

Thus  $F_i(t)^n M \subset M_{f_i}$ . Then it follows from (2.5) that  $M = \sum_{1 \leq i \leq k} M_{f_i}$ .

2° Let  $N$  be another finite  $\Lambda$ -module whose order is a power of  $p$ . If there is a  $\Lambda$ -module isomorphism  $\phi : M \rightarrow N$ , then for each irreducible  $f \in \mathbb{Z}_p[X]$ ,  $\phi|_{M_f} : M_f \rightarrow N_f$  is an isomorphism. Conversely, if  $M_f \cong N_f$  for all irreducible  $f \in \mathbb{Z}_p[X]$ , then by (2.3),  $M \cong N$ .  $\square$

### 3. CLASSIFICATION OF $\Lambda$ -MODULES OF ORDER $p^n$ , $n \leq 4$

#### 3.1. The automorphism group of a finite abelian group.

Let  $p$  be a prime and let  $m \geq n > 0$  be integers. Elements of  $\mathbb{Z}_{p^m}$  can be viewed as elements of  $\mathbb{Z}_{p^n}$  via the homomorphism

$$\begin{aligned} \mathbb{Z}_{p^m} &\longrightarrow \mathbb{Z}_{p^n} \\ a + p^m \mathbb{Z} &\longmapsto a + p^n \mathbb{Z}, \quad a \in \mathbb{Z}. \end{aligned}$$

Likewise, elements of  $p^{m-n} \mathbb{Z}_{p^n}$  can be viewed as elements of  $\mathbb{Z}_{p^m}$  via the embedding

$$\begin{aligned} p^{m-n} \mathbb{Z}_{p^n} &\longrightarrow \mathbb{Z}_{p^m} \\ p^{m-n}(a + p^n \mathbb{Z}) &\longmapsto p^{m-n}a + p^m \mathbb{Z}, \quad a \in \mathbb{Z}. \end{aligned}$$

We shall adopt these conventions hereafter.

Let  $M = \mathbb{Z}_{p^{e_1}}^{n_1} \times \cdots \times \mathbb{Z}_{p^{e_k}}^{n_k}$ , where  $n_i > 0$  and  $e_1 > \cdots > e_k > 0$ . Elements of  $\text{End}_{\mathbb{Z}}(M)$  are of the form

$$\sigma_A : \begin{aligned} M &\longrightarrow M \\ \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} &\longmapsto A \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}, \quad x_i \in \mathbb{Z}_{p^{e_i}}, \end{aligned}$$

where

$$(3.1) \quad A = \begin{bmatrix} A_{11} & p^{e_1-e_2} A_{12} & \cdots & p^{e_1-e_k} A_{1k} \\ A_{21} & A_{22} & \cdots & p^{e_2-e_1} A_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{bmatrix},$$

and  $A_{ij} \in M_{n_i \times n_j}(\mathbb{Z}_{p^{e_i}})$ . Let  $\mathfrak{M}(M)$  denote the set of all matrices of the form (3.1). Then

$$\begin{aligned} \mathfrak{M}(M) &\longrightarrow \text{End}_{\mathbb{Z}}(M) \\ A &\longmapsto \sigma_A \end{aligned}$$

is a ring isomorphism. Let  $\text{GL}(M)$  denote the group of units of  $\mathfrak{M}(M)$ . Of course  $\text{GL}(M) \cong \text{Aut}_{\mathbb{Z}}(M)$  under the above isomorphism. It is known [4, 9] (and also easy to prove) that

$$\text{GL}(M) = \{A : A \text{ is of the form (3.1) with } A_{ii} \in \text{GL}(n_i, \mathbb{Z}_{p^{e_i}}), 1 \leq i \leq k\}.$$

The modulo  $p$  reduction from  $\text{GL}(M)$  to  $\text{GL}(n_1 + \cdots + n_k, \mathbb{Z}_p)$  is denoted by  $\overline{(\cdot)}$ . For each (monic) irreducible  $f \in \mathbb{Z}_p[X]$  with  $f \neq X$ , define

$$\text{GL}(M)_f = \{A \in \text{GL}(M) : \text{the minimal polynomial of}$$

$$\overline{A} \in \text{GL}(n_1 + \cdots + n_k, \mathbb{Z}_p) \text{ is a power of } f\}.$$

If  $\lambda^{(i)} = (\lambda_{i1}, \lambda_{i2}, \dots)$  is a partition of the integer  $n_i / \deg f$ ,  $1 \leq i \leq k$ , we define

$$\begin{aligned} \text{GL}(M)_f^{\lambda^{(1)} \dots \lambda^{(k)}} &= \{A \text{ as in (3.1)} : \text{the elementary divisors of } \overline{A_{ii}} \\ &\text{are } f^{\lambda_{i1}}, f^{\lambda_{i2}}, \dots, 1 \leq i \leq k\}. \end{aligned}$$

In this setting, our goal is to determine the  $\text{GL}(M)$ -conjugacy classes in  $\text{GL}(M)_f$ . We will proceed according to the structure of  $(M, +)$ .

3.2.  $(M, +) = \mathbb{Z}_{p^e}$ .

In this case we must have  $f = X - a$ ,  $a \in \mathbb{Z}_p^\times$ . The conjugacy classes in  $\text{GL}(M)_f$  are represented by

$$[b], \quad b \in \mathbb{Z}_{p^e}, \quad b \equiv a \pmod{p}.$$

3.3.  $(M, +) = \mathbb{Z}_p^n$ .

In this case we must have  $\deg f \mid n$ . The conjugacy classes in  $\text{GL}(M)_f$  are represented by the rational canonical forms in  $\text{GL}(n, \mathbb{Z}_p)$  with elementary divisors  $f^{\lambda_1}, f^{\lambda_2}, \dots$ , where  $\lambda_1 \geq \lambda_2 \geq \dots > 0$  is a partition of  $n/\deg f$ .

3.4.  $(M, +) = \mathbb{Z}_{p^e} \times \mathbb{Z}_p$ ,  $e > 1$ .

In this case,  $\deg f = 1$ .

**Theorem 3.1.** Assume  $(M, +) = \mathbb{Z}_{p^e} \times \mathbb{Z}_p$ ,  $e > 1$ , and  $f = X - a$ ,  $a \in \mathbb{Z}_p^\times$ . The conjugacy classes in  $\text{GL}(M)_f$  are represented by the following matrices:

- (i)  $\begin{bmatrix} b & \\ & b \end{bmatrix} + \begin{bmatrix} p^{e-1}\alpha & 0 \\ 0 & 0 \end{bmatrix}$ ,  $0 < b < p^{e-1}$ ,  $b \equiv a \pmod{p}$ ,  $\alpha \in \mathbb{Z}_p$ .
- (ii)  $\begin{bmatrix} b & \\ & b \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ ,  $0 < b < p^{e-1}$ ,  $b \equiv a \pmod{p}$ .
- (iii)  $\begin{bmatrix} b & \\ & b \end{bmatrix} + \begin{bmatrix} 0 & p^{e-1} \\ \gamma & 0 \end{bmatrix}$ ,  $0 < b < p^{e-1}$ ,  $b \equiv a \pmod{p}$ ,  $\gamma \in \mathbb{Z}_p$ .

*Proof.* Elements of  $\text{GL}(M)_f$  are of the form

$$A(b, \alpha, \beta, \gamma) := \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} p^{e-1}\alpha & p^{e-1}\beta \\ \gamma & 0 \end{bmatrix},$$

where  $0 < b < p^{e-1}$ ,  $b \equiv a \pmod{p}$ ,  $\alpha, \beta, \gamma \in \mathbb{Z}_p$ . Let  $A(b, \alpha, \beta, \gamma), A(b, \alpha', \beta', \gamma') \in \text{GL}(M)_f$  and

$$P = \begin{bmatrix} x & p^{e-1}y \\ z & w \end{bmatrix} \in \text{GL}(M), \quad x \in \mathbb{Z}_{p^e}^\times, \quad w \in \mathbb{Z}_p^\times, \quad y, z \in \mathbb{Z}_p.$$

The equation  $PA(b, \alpha, \beta, \gamma) = A(b, \alpha', \beta', \gamma')P$  is equivalent to

$$\begin{bmatrix} p^{e-1}(x\alpha + y\gamma) & p^{e-1}x\beta \\ w\gamma & 0 \end{bmatrix} = \begin{bmatrix} p^{e-1}(\alpha'x + \beta'z) & p^{e-1}\beta'w \\ \gamma'x & 0 \end{bmatrix}.$$

The above equation can be written as a matrix equation over  $\mathbb{Z}_p$ :

$$\begin{bmatrix} x\alpha + y\gamma & x\beta \\ w\gamma & 0 \end{bmatrix} = \begin{bmatrix} \alpha'x + \beta'z & \beta'w \\ \gamma'x & 0 \end{bmatrix},$$

equivalently,

$$\begin{bmatrix} x & y \\ 0 & w \end{bmatrix} \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix} = \begin{bmatrix} \beta' & \alpha' \\ 0 & \gamma' \end{bmatrix} \begin{bmatrix} w & z \\ 0 & x \end{bmatrix}.$$

So,  $A(b, \alpha, \beta, \gamma)$  and  $A(b, \alpha', \beta', \gamma')$  are conjugate if and only if there exist  $x, y \in \mathbb{Z}_p^\times$  and  $y, z \in \mathbb{Z}_p$  such that

$$(3.2) \quad \begin{bmatrix} x & y \\ 0 & w \end{bmatrix} \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix} \begin{bmatrix} w^{-1} & z \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} \beta' & \alpha' \\ 0 & \gamma' \end{bmatrix}.$$

Let  $\mathcal{M} = \left\{ \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_p \right\}$ . For  $A = \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix}$ ,  $A' = \begin{bmatrix} \beta' & \alpha' \\ 0 & \gamma' \end{bmatrix} \in \mathcal{M}$ , say  $A \sim A'$  if (3.2) is satisfied for some  $x, w \in \mathbb{Z}_p^\times$  and  $y, z \in \mathbb{Z}_p$ . It is easy to see that the  $\sim$  equivalence classes in  $\mathcal{M}$  are represented by

- (i)  $\begin{bmatrix} 0 & \alpha \\ 0 & 0 \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p,$
- (ii)  $\begin{bmatrix} 0 & \\ & 1 \end{bmatrix},$
- (iii)  $\begin{bmatrix} 1 & \\ & \gamma \end{bmatrix}, \quad \gamma \in \mathbb{Z}_p.$

These matrices correspond to the representatives of the conjugacy classes in  $\mathrm{GL}(M)_f$  stated in the theorem.  $\square$

3.5.  $(M, +) = \mathbb{Z}_{p^2}^2$ .

In this case,  $\deg f = 1$  or  $2$ .

**Theorem 3.2.** *Assume  $(M, +) = \mathbb{Z}_{p^2}^2$ .*

- (i) *Let  $f = X - a$ ,  $a \in \mathbb{Z}_p^\times$ . Then the conjugacy classes in  $\mathrm{GL}(M)_f^{(1,1)}$  are represented by the following matrices:*

$$(i.1) \quad \begin{bmatrix} b & \\ & b \end{bmatrix} + p \begin{bmatrix} \alpha & \\ & \delta \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad 0 \leq \alpha \leq \delta < p.$$

$$(i.2) \quad \begin{bmatrix} b & \\ & b \end{bmatrix} + p \begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha \in \mathbb{Z}_p.$$

$$(i.3) \quad \begin{bmatrix} b & \\ & b \end{bmatrix} + p \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irreducible.}$$

- (ii) *Let  $f = X - a$ ,  $a \in \mathbb{Z}_p^\times$ . Then the conjugacy class in  $\mathrm{GL}(M)_f^{(2)}$  are represented by*

$$\begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} + p \begin{bmatrix} \alpha & 0 \\ \gamma & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha, \gamma \in \mathbb{Z}_p.$$

- (iii) *Let  $f = X^2 + a_1X + a_0 \in \mathbb{Z}_p[X]$  be irreducible. Then the conjugacy classes in  $\mathrm{GL}(M)_f$  are represented by*

$$\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}, \quad 0 \leq b_0, b_1 < p, \quad b_0 \equiv a_0 \pmod{p}, \\ b_1 \equiv a_1 \pmod{p}, \quad \alpha, \beta \in \mathbb{Z}_p.$$

*Proof.* We remind the reader that in the proof, our notation is local in each of the three cases.

- (i) Elements of  $\mathrm{GL}(M)_f^{(1,1)}$  are of the form

$$A(b, \alpha, \beta, \gamma, \delta) := \begin{bmatrix} b & \\ & b \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.$$

Clearly,  $A(b, \alpha, \beta, \gamma, \delta)$  and  $A(b, \alpha', \beta', \gamma', \delta')$  are conjugate in  $\mathrm{GL}(M)$  if and only if  $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$  and  $\begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}$  are conjugate in  $M_{2 \times 2}(\mathbb{Z}_p)$ . The conjugacy classes in  $M_{2 \times 2}(\mathbb{Z}_p)$  are represented by

- (1)  $\begin{bmatrix} \alpha & \\ & \delta \end{bmatrix}, \quad 0 \leq \alpha \leq \delta < p,$
- (2)  $\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p,$

$$(3) \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix}, \quad X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irreducible.}$$

These correspond to the matrices in (i.1) – (i.3).

(ii) Elements of  $\text{GL}(M)_f^{(2)}$  are conjugate to matrices of the form

$$A(b, \alpha, \beta, \gamma, \delta) := \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.$$

Assume that  $P \in \text{GL}(M) = \text{GL}(2, \mathbb{Z}_{p^2})$  such that

$$(3.3) \quad PA(b, \alpha, \beta, \gamma, \delta) = A(b, \alpha', \beta', \gamma', \delta')P.$$

Then over  $\mathbb{Z}_p$ ,

$$\overline{P} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \overline{P},$$

which implies that  $\overline{P} = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}$ ,  $c \in \mathbb{Z}_p^\times$ ,  $d \in \mathbb{Z}_p$ . So

$$P = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \quad x, y, z, w \in \mathbb{Z}_p.$$

Now (3.3) becomes

$$p \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = p \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + p \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}.$$

Over  $\mathbb{Z}_p$ , this becomes

$$\begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix},$$

which can be simplified as

$$\begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + \begin{bmatrix} z & w - x \\ 0 & -z \end{bmatrix}.$$

Thus,  $A(b, \alpha, \beta, \gamma, \delta)$  and  $A(b, \alpha', \beta', \gamma', \delta')$  are conjugate if and only if there exist  $d, z, w \in \mathbb{Z}_p$  such that

$$(3.4) \quad \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & -d \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} z & w \\ 0 & -z \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}.$$

For  $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ ,  $A' = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \in \text{M}_{2 \times 2}(\mathbb{Z}_p)$ , say  $A \sim A'$  if (3.4) is satisfied for some  $d, z, w \in \mathbb{Z}_p$ . It is easy to see that the  $\sim$  equivalence classes in  $\text{M}_{2 \times 2}(\mathbb{Z}_p)$  are represented by

$$\begin{bmatrix} \alpha & 0 \\ \gamma & 0 \end{bmatrix}, \quad \alpha, \beta \in \mathbb{Z}_p,$$

which correspond to the matrices in (ii).

(iii) Elements of  $\text{GL}(M)_f$  are conjugate to matrices of the form

$$A(f, \alpha, \beta, \gamma, \delta) := \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 \leq b_0, b_1 < p, \quad b_0 \equiv a_0 \pmod{p}, \\ b_1 \equiv a_1 \pmod{p}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.$$

Assume that  $P \in \text{GL}(2, \mathbb{Z}_{p^2})$  such that

$$(3.5) \quad PA(f, \alpha, \beta, \gamma, \delta) = A(f, \alpha', \beta', \gamma', \delta')P.$$

Then over  $\mathbb{Z}_p$ ,

$$\overline{P} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \overline{P},$$

which implies that

$$P = uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \quad 0 \leq u, v < p, (u, v) \neq (0, 0), x, y, z, w \in \mathbb{Z}_p.$$

Now (3.5) becomes the following equation over  $\mathbb{Z}_p$ :

$$(3.6) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) + \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} - \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix}.$$

The space  $\left\{ \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} X - X \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} : X \in M_{2 \times 2}(\mathbb{Z}_p) \right\}$  has dimension 2 over  $\mathbb{Z}_p$  [5, §4.4] and has a basis

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} &= \begin{bmatrix} 0 & -1 \\ -b_0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} &= \begin{bmatrix} b_0 & b_1 \\ 0 & -b_0 \end{bmatrix}. \end{aligned}$$

So (3.6) can be written as

$$(3.7) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) + \begin{bmatrix} -d & \frac{c}{b_0} - d\frac{b_1}{b_0} \\ c & d \end{bmatrix}, \quad c, d \in \mathbb{Z}_p.$$

Thus  $A(f, \alpha, \beta, \gamma, \delta)$  and  $A(f, \alpha', \beta', \gamma', \delta')$  are conjugate if and only if there exist  $0 \leq u, v < p$ ,  $(u, v) \neq (0, 0)$ , and  $c, d \in \mathbb{Z}_p$  such that

$$(3.8) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \left( \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} - \begin{bmatrix} -d & \frac{c}{b_0} - d\frac{b_1}{b_0} \\ c & d \end{bmatrix} \right) \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right)^{-1} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}.$$

For  $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ ,  $A' = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \in M_{2 \times 2}(\mathbb{Z}_p)$ , say  $A \sim A'$  if (3.8) is satisfied for some  $0 \leq u, v < p$ ,  $(u, v) \neq (0, 0)$ , and  $c, d \in \mathbb{Z}_p$ . It remains to show that the  $\sim$  equivalence classes in  $M_{2 \times 2}(\mathbb{Z}_p)$  are represented by

$$\begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}, \quad \alpha, \beta \in \mathbb{Z}_p.$$

First, choose  $u = 1$ ,  $v = 0$ ,  $c = -\gamma$ ,  $d = -\delta$ . Then the left side of (3.8) becomes  $\begin{bmatrix} \alpha' & \beta' \\ 0 & 0 \end{bmatrix}$  for some  $\alpha', \beta' \in \mathbb{Z}_p$ .

Next, assume that (3.8) holds with  $\gamma = \delta = \gamma' = \delta' = 0$ . We want to show that  $(\alpha, \beta) = (\alpha', \beta')$ . Taking the traces of the two sides of (3.8), we have  $\alpha = \alpha'$ . Now (3.7) with  $\alpha = \alpha'$  and  $\gamma = \delta = \gamma' = \delta' = 0$  gives

$$\begin{bmatrix} u\alpha & u\beta \\ -vb_0\alpha & -vb_0\beta \end{bmatrix} = \begin{bmatrix} \alpha u - \beta' v b_0 & \alpha v - \beta'(u - v b_1) \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} -d & \frac{c}{b_0} - d\frac{b_1}{b_0} \\ c & d \end{bmatrix}.$$



Taking the traces, we have  $vb_0\beta = vb_0\beta'$ . If  $v \neq 0$ , then  $\beta = \beta'$ . If  $v = 0$ , then  $c = d = 0$ , which implies  $u\beta = u\beta'$ . Since  $u \neq 0$ , we also have  $\beta = \beta'$ .  $\square$

3.6.  $(M, +) = \mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$ .

In this case  $\deg f = 1$ .

**Theorem 3.3.** Assume  $(M, +) = \mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$  and  $f = X - a$ ,  $a \in \mathbb{Z}_p^\times$ .

(i) The conjugacy classes in  $\mathrm{GL}(M)_f^{(1)(1,1)}$  are represented by the following matrices:

$$(i.1) \quad \begin{bmatrix} b & & \\ & b & \\ & & b \end{bmatrix} + \begin{bmatrix} p\alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha \in \mathbb{Z}_p.$$

$$(i.2) \quad \begin{bmatrix} b & & \\ & b & \\ & & b \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}.$$

$$(i.3) \quad \begin{bmatrix} b & & \\ & b & \\ & & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 0 & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \eta \in \mathbb{Z}_p.$$

$$(i.4) \quad \begin{bmatrix} b & & \\ & b & \\ & & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}.$$

(ii) The conjugacy classes in  $\mathrm{GL}(M)_f^{(1)(2)}$  are represented by the following matrices:

$$(ii.1) \quad \begin{bmatrix} b & & \\ & b & 1 \\ & & b \end{bmatrix} + \begin{bmatrix} p\alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha \in \mathbb{Z}_p.$$

$$(ii.2) \quad \begin{bmatrix} b & & \\ & b & 1 \\ & & b \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}.$$

$$(ii.3) \quad \begin{bmatrix} b & & \\ & b & 1 \\ & & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 0 & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \eta \in \mathbb{Z}_p.$$

*Proof.* (i) Elements of  $\mathrm{GL}(M)_f^{(1)(1,1)}$  are of the form

$$A(b, \alpha, \dots, \eta) := \begin{bmatrix} b & & \\ & b & \\ & & b \end{bmatrix} + \begin{bmatrix} p\alpha & p\beta & p\gamma \\ \delta & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha, \dots, \eta \in \mathbb{Z}_p.$$

Assume that  $P \in \mathrm{GL}(M)$  such that

$$(3.9) \quad PA(b, \alpha, \dots, \eta) = A(b, \alpha', \dots, \eta')P.$$

Write

$$P = \begin{bmatrix} x & pY \\ Z & W \end{bmatrix},$$

where  $x \in \mathbb{Z}_p^\times$ ,  $Y \in M_{1 \times 2}(\mathbb{Z}_p)$ ,  $Z \in M_{2 \times 1}(\mathbb{Z}_p)$ ,  $W \in GL(2, \mathbb{Z}_p)$ . Then (3.9) becomes

$$\begin{bmatrix} px\alpha + pY \begin{bmatrix} \delta \\ \eta \end{bmatrix} & px[\beta, \gamma] \\ W \begin{bmatrix} \delta \\ \eta \end{bmatrix} & 0 \end{bmatrix} = \begin{bmatrix} p\alpha'x + p[\beta', \gamma']z & p[\beta', \gamma']W \\ \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} x & 0 \end{bmatrix}.$$

Over  $\mathbb{Z}_p$ , this becomes

$$\begin{bmatrix} x\alpha + Y \begin{bmatrix} \delta \\ \eta \end{bmatrix} & x[\beta, \gamma] \\ W \begin{bmatrix} \delta \\ \eta \end{bmatrix} & 0 \end{bmatrix} = \begin{bmatrix} \alpha'x + [\beta', \gamma']z & [\beta', \gamma']W \\ \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} x & 0 \end{bmatrix}.$$

It is more convenient to write the above equation as

$$\begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix} \begin{bmatrix} W & Z \\ 0 & x \end{bmatrix}.$$

So,  $A(b, \alpha, \dots, \eta)$  and  $A(b, \alpha', \dots, \eta')$  are conjugate if and only if

$$(3.10) \quad \begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} \begin{bmatrix} W^{-1} & Z \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix}$$

for some  $x \in \mathbb{Z}_p^\times$ ,  $W \in GL(2, \mathbb{Z}_p)$ ,  $Y \in M_{1 \times 2}(\mathbb{Z}_p)$ ,  $Z \in M_{2 \times 1}(\mathbb{Z}_p)$ .

Let

$$\mathcal{M} = \left\{ \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} : \alpha, \dots, \eta \in \mathbb{Z}_p \right\}.$$

For

$$A = \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix}, \quad A' = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix} \in \mathcal{M},$$

say  $A \sim A'$  if (3.10) is satisfied. It is easy to see that the  $\sim$  equivalence classes in  $\mathcal{M}$  are represented by

$$(1) \quad \begin{bmatrix} [0 \ 0] & \alpha \\ & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p,$$

$$(2) \quad \begin{bmatrix} [0 \ 0] & \\ & \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix},$$

$$(3) \quad \begin{bmatrix} [1 \ 0] & \\ & \begin{bmatrix} 0 \\ \eta \end{bmatrix} \end{bmatrix}, \quad \eta \in \mathbb{Z}_p,$$

$$(4) \quad \begin{bmatrix} [1 \ 0] & \\ & \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix}.$$

These correspond to the matrices in (i.1) – (i.4).

(ii) Elements of  $\text{GL}(M)_f^{(1)(1,1)}$  are conjugate for matrices of the form

$$A(b, \alpha, \dots, \eta) := \begin{bmatrix} b & & \\ & b & 1 \\ & & b \end{bmatrix} + \begin{bmatrix} p\alpha & p\beta & p\gamma \\ \delta & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \quad b \equiv a \pmod{p}, \quad \alpha, \dots, \eta \in \mathbb{Z}_p.$$

Assume that  $P \in \text{GL}(M)$  such that

$$(3.11) \quad PA(b, \alpha, \dots, \eta) = A(b, \alpha', \dots, \eta')P.$$

Write

$$P = \begin{bmatrix} x & pY \\ Z & W \end{bmatrix},$$

where  $x \in \mathbb{Z}_p^\times$ ,  $Y \in M_{1 \times 2}(\mathbb{Z}_p)$ ,  $Z \in M_{2 \times 1}(\mathbb{Z}_p)$ ,  $W \in \text{GL}(2, \mathbb{Z}_p)$ . Since  $W$  commutes with  $\begin{bmatrix} b & 1 \\ & b \end{bmatrix}$ , we have  $W = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}$ . Equation (3.11) is equivalent to

$$\begin{aligned} & \begin{bmatrix} 0 & pY \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \\ 0 & W \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{bmatrix} + \begin{bmatrix} px\alpha + pY \begin{bmatrix} \delta \\ \eta \end{bmatrix} & px[\beta, \gamma] \\ W \begin{bmatrix} \delta \\ \eta \end{bmatrix} & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} Z & \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} W \end{bmatrix} + \begin{bmatrix} p\alpha'x + p[\beta', \gamma']Z & p[\beta', \gamma']W \\ \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} x & 0 \end{bmatrix}. \end{aligned}$$

Over  $\mathbb{Z}_p$ , this becomes

$$\begin{bmatrix} 0 & Y \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} x\alpha + Y \begin{bmatrix} \delta \\ \eta \end{bmatrix} & x[\beta, \gamma] \\ W \begin{bmatrix} \delta \\ \eta \end{bmatrix} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} Z & 0 \end{bmatrix} + \begin{bmatrix} \alpha'x + [\beta', \gamma']Z & [\beta', \gamma']W \\ \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} x & 0 \end{bmatrix},$$

which can be written as

$$\begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} + \begin{bmatrix} Y \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & 0 \\ 0 & -\begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} Z \end{bmatrix} = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix} \begin{bmatrix} W & Z \\ 0 & x \end{bmatrix}.$$

So,  $A(b, \alpha, \dots, \eta)$  and  $A(b, \alpha', \dots, \eta')$  are conjugate if and only if

(3.12)

$$\begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} \begin{bmatrix} W^{-1} & Z \\ 0 & x^{-1} \end{bmatrix} + \begin{bmatrix} Y \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} W^{-1} & Y \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} Z \\ 0 & \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} WZ \end{bmatrix} = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix}$$

for some  $x \in \mathbb{Z}_p^\times$ ,  $Y \in M_{1 \times 2}(\mathbb{Z}_p)$ ,  $Z \in M_{2 \times 1}(\mathbb{Z}_p)$ ,  $W = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \in \text{GL}(2, \mathbb{Z}_p)$ .

Let

$$\mathcal{M} = \left\{ \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} : \alpha, \dots, \eta \in \mathbb{Z}_p \right\}.$$

For

$$A = \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix}, \quad A' = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \begin{bmatrix} \delta' \\ \eta' \end{bmatrix} \end{bmatrix} \in \mathcal{M},$$

say  $A \sim A'$  if (3.12) is satisfied. It remains to determine the representatives of the  $\sim$  equivalence classes in  $\mathcal{M}$ .

In (3.12), we may assume  $W = \begin{bmatrix} 1 & d \\ & 1 \end{bmatrix}$  by replacing  $x, Y, W, Z$  with  $\frac{1}{c}x, \frac{1}{c}Y, \frac{1}{c}W, cZ$ , respectively. Let  $Y = [y_1, y_2]$ ,  $Z = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$ . Then (3.12) becomes

$$(3.13) \quad \begin{bmatrix} x\beta & -x\beta d + x\gamma + y_1 & \alpha + x\beta z_1 + x\gamma z_2 + y_1\delta x^{-1} + y_2\eta x^{-1} + y_1 z_2 \\ 0 & 0 & \delta x^{-1} + d\eta x^{-1} + z_2 \\ 0 & 0 & \eta x^{-1} \end{bmatrix} = \begin{bmatrix} \beta' & \gamma' & \alpha' \\ 0 & 0 & \delta' \\ 0 & 0 & \eta' \end{bmatrix}.$$

We claim that the  $\sim$  equivalence classes in  $\mathcal{M}$  are represented by

$$(1) \quad \begin{bmatrix} [0 \ 0] & \alpha \\ & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p,$$

$$(2) \quad \begin{bmatrix} [0 \ 0] & 0 \\ & \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix},$$

$$(3) \quad \begin{bmatrix} [1 \ 0] & 0 \\ & \begin{bmatrix} 0 \\ \eta \end{bmatrix} \end{bmatrix}, \quad \eta \in \mathbb{Z}_p.$$

The proof of (ii) will be complete when this claim is proved.

First, it is clear that matrices from different families of (1) – (3) are not  $\sim$  equivalent. So it remains to show that every  $A \in \mathcal{M}$  can be brought into one of the “canonical forms” in (1) – (3) through  $\sim$  equivalence, and the entries in the canonical form are uniquely determined by  $A$ .

Let

$$A = \begin{bmatrix} [\beta, \gamma] & \alpha \\ & \begin{bmatrix} \delta \\ \eta \end{bmatrix} \end{bmatrix} \in \mathcal{M}.$$

First assume  $\beta = 0$  and  $\eta = 0$ . Then

$$\text{LHS of (3.13)} = \begin{bmatrix} [0 \ 0] & \alpha' \\ 0 & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \end{bmatrix}$$

if and only if

$$(3.14) \quad \begin{cases} x\gamma + y_1 = 0, \\ \delta x^{-1} + z_2 = 0, \end{cases}$$

and

$$(3.15) \quad \alpha' = \alpha + \gamma\delta.$$

System (3.14) has a solution  $(x, y_1, z_2) = (1, -\gamma, -\delta)$ . Equation (3.15) shows that  $\alpha'$  is uniquely determined by  $A$ .

Next, assume  $\beta = 0$  and  $\eta \neq 0$ . Then

$$\text{LHS of (3.13)} = \begin{bmatrix} [0 \ 0] & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \end{bmatrix}$$

if and only if

$$(3.16) \quad \begin{cases} x\gamma + y_1 = 0, \\ \alpha + x\gamma z_2 + y_1\delta x^{-1} + y_2\eta x^{-1} + y_1 z_2 = 0, \\ \delta x^{-1} + d\eta x^{-1} + z_2 = 0, \\ \eta x^{-1} = 1. \end{cases}$$

System (3.16) has a solution  $(d, x, y_1, y_2, z_2)$ . (Let  $d$  be arbitrary. Solve for  $x$  from the last equation,  $y_1$  from the first equation,  $z_2$  from the third equation, and  $y_2$  from the second equation.)

Finally, assume  $\beta \neq 0$ . Then

$$\text{LHS of (3.13)} = \begin{bmatrix} [1 \ 0] & \begin{bmatrix} 0 \\ 0 \\ \eta' \end{bmatrix} \end{bmatrix}$$

if and only if

$$(3.17) \quad \begin{cases} x\beta = 1, \\ -x\beta d + x\gamma + y_1 = 0, \\ \alpha + x\beta z_1 + x\gamma z_2 + y_1\delta x^{-1} + y_2\eta x^{-1} + y_1 z_2 = 0, \\ \delta x^{-1} + d\eta x^{-1} + z_2 = 0, \end{cases}$$

and

$$(3.18) \quad \eta' = \eta\beta.$$

System (3.17) has a solution  $(d, x, y_1, y_2, z_1, z_2)$ . (Let  $y_1$  and  $y_2$  be arbitrary. Solve for  $x$  from the first equation,  $d$  from the second equation,  $z_2$  from the last equation, and  $z_1$  from the third equation.) Equation (3.18) shows that  $\eta'$  is uniquely determined by  $A$ .  $\square$

### 3.7. Classification of $\Lambda$ -modules of order $p^n$ , $n \leq 4$ .

The classification of  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$ , is obtained by combining the results in 3.2 – 3.6 and using Theorem 2.1. A complete description of the classification is given in Table 1 in the appendix. From Table 1 we find that the number of nonisomorphic  $\Lambda$ -modules of order  $p^n$  is

$$(3.19) \quad \begin{cases} 1 & \text{if } n = 0, \\ p - 1 & \text{if } n = 1, \\ 2p^2 - p - 1 & \text{if } n = 2, \\ 3p^3 - 2p^2 - 1 & \text{if } n = 3, \\ 5p^4 - 2p^3 - 2p - 1 & \text{if } n = 4. \end{cases}$$

## 4. FINITE ALEXANDER QUANDLES

By Theorem 1.1, the classification of finite Alexander quandles  $M$  is the same as the classification of finite  $\Lambda$ -modules of the form  $(1-t)M$ . First, the following question has to be answered: Given a finite  $\Lambda$ -module  $N$  and an integer  $l > 0$ , does there exist a  $\Lambda$ -module  $M \supset N$  such that  $(1-t)M = N$  and  $|M/N| = l$ ? Assume that such an  $M$  exists. Since

$$M/(1-t)M \xrightarrow{1-t} (1-t)M/(1-t)^2M = N/(1-t)N$$

is an onto  $\Lambda$ -map, we have  $|N/(1-t)N| \mid l$ . We will see in Theorem 4.3 that  $|N/(1-t)N| \mid l$  is also a sufficient condition for the existence of  $M$ .

**Lemma 4.1.** *Let  $N \subset M$  be abelian groups and let  $\alpha : N \rightarrow N$  and  $\bar{\alpha} : M \rightarrow N$  be  $\mathbb{Z}$ -maps such that  $\bar{\alpha}|_N = \alpha$ . If  $1 - \alpha \in \text{Aut}(N)$ , then  $1 - \bar{\alpha} \in \text{Aut}(M)$ .*

*Proof.* We first show that  $1 - \bar{\alpha}$  is 1-1. Let  $x \in \ker(1 - \bar{\alpha})$ . Then

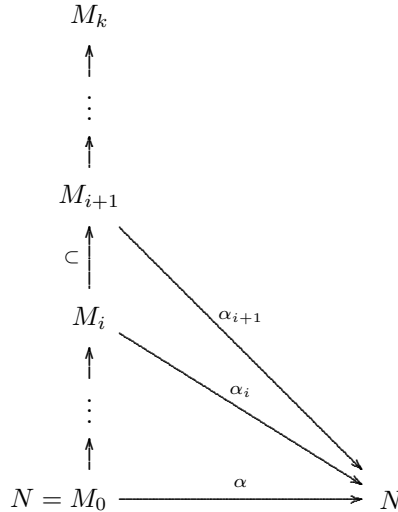
$$0 = \bar{\alpha}(0) = \bar{\alpha}(x - \bar{\alpha}(x)) = \bar{\alpha}(x) - \alpha(\bar{\alpha}(x)) = (1 - \alpha)(\bar{\alpha}(x)).$$

Since  $1 - \alpha \in \text{Aut}(N)$ , we have  $\bar{\alpha}(x) = 0$ . Thus  $x = [(1 - \bar{\alpha}) + \bar{\alpha}](x) = 0$ .

Now we show that  $1 - \bar{\alpha} : M \rightarrow M$  is onto. Let  $y \in M$ . Since  $\bar{\alpha}(y) \in N$  and  $1 - \alpha \in \text{Aut}(N)$ , there exists  $x \in N$  such that  $(1 - \alpha)(x) = \bar{\alpha}(y)$ . Then  $y = y - \bar{\alpha}(y) + x - \alpha(x) = (1 - \bar{\alpha})(y + x)$ .  $\square$

**Theorem 4.2.** *Let  $N$  be a finite abelian group and  $\alpha \in \text{End}_{\mathbb{Z}}(N)$ . Then there exist a finite abelian group  $M \supset N$  with  $|M/N| = |N/\alpha(N)|$  and an onto homomorphism  $\bar{\alpha} : M \rightarrow N$  such that  $\bar{\alpha}|_N = \alpha$ .*

*Proof.* We may assume that  $N$  is a finite abelian  $p$ -group. If  $\alpha(N) = N$ , there is nothing to prove. So assume  $\alpha(N) \neq N$ . Let  $|N/\alpha(N)| = p^k$  and  $\text{rank } N = r$  (the number of cyclic summands in a decomposition of  $N$ ). We will inductively construct finite abelian  $p$ -groups  $N = M_0 \subset M_1 \subset \cdots \subset M_k$  and  $\mathbb{Z}$ -maps  $\alpha_i : M_i \rightarrow N$ ,  $0 \leq i \leq k$ , such that  $\alpha_0 = \alpha$ ,  $|M_{i+1}/M_i| = |\alpha_{i+1}(M_{i+1})/\alpha_i(M_i)| = p$ ,  $\text{rank } M_i = r$ , and  $\alpha_{i+1}|_{M_i} = \alpha_i$ . Then  $M = M_k$  and  $\bar{\alpha} = \alpha_k$  have the desired property.



Let  $0 \leq i < k$  and assume that  $M_i$  and  $\alpha_i$  have been constructed. We now construct  $M_{i+1}$  and  $\alpha_{i+1}$ .

We claim that the mapping  $M_i/pM_i \rightarrow N/pN$  induced by  $\alpha_i$  is not 1-1. Otherwise, since  $|M_i/pM_i| = p^r = |N/pN|$ , the mapping is also onto. Then for each  $x \in N$ , there exist  $y_0 \in M_i$  and  $x_0 \in N$  such that

$$x = \alpha_i(y_0) + px_0.$$

In the same way,  $x_0 = \alpha_i(y_1) + px_1$  for some  $y_1 \in M_i$  and  $x_1 \in N$ . Continuing this way, we can write

$$x = \alpha_i(y_0 + py_1 + \cdots + p^n y_n) + p^{n+1}x_n, \quad y_0, \dots, y_n \in M_i, \quad x_n \in N.$$

Choose  $n$  large enough such that  $p^{n+1}x_n = 0$ . Then  $x = \alpha_i(y_0 + py_1 + \cdots + p^n y_n) \in \alpha_i(M_i)$ . So  $N = \alpha_i(M_i)$ , which is a contradiction since  $|\alpha_i(M_i)/\alpha(N)| = p^i < p^k = |N/\alpha(N)|$ .

By the above claim, there exists  $a \in M_i \setminus pM_i$  such that  $\alpha_i(a) \in pN$ . Write  $\alpha_i(a) = pb$  for some  $b \in N$ .

**Case 1.** Assume  $b \notin \alpha_i(M_i)$ . Write  $M_i = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_r}}$ ,  $e_1 \geq \cdots \geq e_r > 0$ . Since  $a \in M_i \setminus pM_i$ , we may assume  $a = (pw, 1, 0)$ , where  $w \in \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_{s-1}}}$  for some  $0 \leq s < r$ . Let  $M_{i+1} = A \times \mathbb{Z}_{p^{e_{s+1}}} \times B$  where  $A = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_{s-1}}}$ ,  $B = \mathbb{Z}_{p^{e_{s+1}}} \times \cdots \times \mathbb{Z}_{p^{e_r}}$ . Define  $\mathbb{Z}$ -maps

$$\begin{aligned} \iota: \quad M_i = A \times \mathbb{Z}_{p^{e_s}} \times B &\longrightarrow M_{i+1} = A \times \mathbb{Z}_{p^{e_{s+1}}} \times B \\ (x, y, z) &\longmapsto (x, py, z) \\ \\ \alpha_{i+1}: \quad M_{i+1} = A \times \mathbb{Z}_{p^{e_{s+1}}} \times B &\longrightarrow N \\ (x, y, z) &\longmapsto \alpha_i(x, 0, z) + y(b - \alpha_i(w, 0, 0)) \end{aligned}$$

Then  $\iota$  is 1-1,  $\alpha_{i+1}\iota = \alpha_i$ , and  $|M_{i+1}/M_i| = p = |\alpha_{i+1}(M_{i+1})/\alpha_i(M_i)|$ .

**Case 2.** Assume  $b \in \alpha_i(M_i)$ , say,  $b = \alpha_i(c)$ ,  $c \in M_i$ . Then  $\alpha_i(a) = p\alpha_i(c)$ . Let  $a_1 = a - pc$ . Then  $a_1 \in M_i \setminus pM_i$  and  $\alpha_i(a_1) = 0$ . Choose  $b' \in N \setminus \alpha_i(M_i)$  such that  $pb' \in \alpha_i(M_i)$ . Write  $pb' = \alpha_i(d)$ ,  $d \in M_i$ . Choose  $\epsilon = 0$  or  $1$  such that  $a' := d + \epsilon a_1 \notin pM_i$ . Then  $\alpha_i(a') = pb'$ . Now we are in Case 1 with  $a', b'$  in place of  $a, b$ , respectively.  $\square$

**Theorem 4.3.** *Let  $N$  be a finite  $\Lambda$ -module with  $|N/(1-t)N| = l$ . Then there exists a finite  $\Lambda$ -module  $M \supset N$  with  $|M/N| = l$  and  $(1-t)M = N$ .*

*Proof.* Let  $\alpha = 1-t \in \text{End}_{\mathbb{Z}}(N)$ . By Theorem 4.2, there exist a finite abelian group  $M \supset N$  and an onto  $\mathbb{Z}$ -map  $\bar{\alpha}: M \rightarrow N$  such that  $\bar{\alpha}|_N = \alpha$  and  $|M/N| = |N/\alpha(N)|$ . Since  $1-\alpha \in \text{Aut}_{\mathbb{Z}}(N)$ , by Lemma 4.1,  $1-\bar{\alpha} \in \text{Aut}_{\mathbb{Z}}(M)$ . Make  $M$  into a  $\Lambda$ -module by defining

$$tx = (1 - \bar{\alpha})(x), \quad x \in M.$$

Then  ${}_{\Lambda}N$  is a submodule of  ${}_{\Lambda}M$  and  $(1-t)M = \bar{\alpha}(M) = N$ .  $\square$

**Corollary 4.4.** *Let  $p$  be a prime and  $n$  a positive integer. Let  $\mathcal{M}_{p^n}$  be a complete set of nonisomorphic  $\Lambda$ -modules  $N$  such that  $|N| = p^i$ ,  $|(1-t)N| = p^j$ ,  $2i-j \leq n$ . For each  $N \in \mathcal{M}_{p^n}$ , let  $M_N \supset N$  be a  $\Lambda$ -module with  $|M_N| = p^n$  and  $(1-t)M_N = N$ . (The existence of  $M_N$  is guaranteed by Theorem 4.3.) Then  $\{(M_N, *) : N \in \mathcal{M}_{p^n}\}$  is a complete set of nonisomorphic Alexander quandles of order  $p^n$ .*

*Proof.* Given a  $\Lambda$ -module  $N$  with  $|N| = p^i$  and  $|(1-t)N| = p^j$ , it follows from Theorem 4.3 that  $n \geq 2i - j$  is a necessary and sufficient condition on  $n$  for which there exists a  $\Lambda$ -module  $M \supset N$  with  $|M| = p^n$  and  $(1-t)M = N$ . Now the conclusion in the corollary follows from Theorem 1.1.  $\square$

The  $\Lambda$ -modules in  $\mathcal{M}_{p^n}$ ,  $n \leq 4$ , are contained in Table 1; to save space, we will not enumerate these modules separately. From Table 1 we find that the number of nonisomorphic Alexander quandles of order  $p^n$  ( $n \leq 4$ ) is

$$(4.1) \quad \begin{cases} 1 & \text{if } n = 0, \\ p - 1 & \text{if } n = 1, \\ 2p^2 - 2p - 1 & \text{if } n = 2, \\ 3p^3 - 4p^2 + p - 3 & \text{if } n = 3, \\ 5p^4 - 6p^3 + p^2 - 6p - 1 & \text{if } n = 4. \end{cases}$$

The number of nonisomorphic connected Alexander quandles of order  $p^n$  ( $n \leq 4$ ), also from Table 1, is

$$(4.2) \quad \begin{cases} 1 & \text{if } n = 0, \\ p - 2 & \text{if } n = 1, \\ 2p^2 - 3p - 1 & \text{if } n = 2, \\ 3p^3 - 6p^2 + p & \text{if } n = 3, \\ 5p^4 - 9p^3 + p^2 - 2p + 1 & \text{if } n = 4. \end{cases}$$

**Remark.**

- (i) (4.1) agrees with the numbers of nonisomorphic Alexander quandles of order  $\leq 15$  in [8].
- (ii) (4.2) with  $n = 2$  agrees with the results of [3, 8]; (4.2) with  $p^n = 2^4$  agrees with the number in [7].
- (iii) [7] stated that the number of nonisomorphic Alexander quandles of order 16 is 24. Our result ((4.1) with  $p^n = 2^4$ ) is 23. It appears that the two Alexander quandles in [7] with  $\text{Im}(\text{Id} - \phi) = \mathbb{Z}_4 \oplus \mathbb{Z}_2$  (notation of [7]) are isomorphic. Professor W. E. Clark computed the numbers of nonisomorphic quandles of order  $p^n < 2^8$  using a computer program; his results (with  $n \leq 4$ ) agree with (4.1).

APPENDIX: TABLE

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$

$n = 0$				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
0	[0]	1	1	1
$n = 1$				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_p$	$[b], b \in \mathbb{Z}_p^\times$	$p^0$ if $b = 1$	1	$p - 1$
		$p^1$ if $b \neq 1$	$p - 2$	



## ACKNOWLEDGMENT

I thank Professor W. Edwin Clark for sharing his computational results on the numbers of nonisomorphic Alexander quandles.

## REFERENCES

- [1] S. Carter, S. Kamada, M. Saito, *Surfaces in 4-Space*, Encyclopaedia of Mathematical Sciences, 142. Low-Dimensional Topology, III. Springer-Verlag, Berlin, 2004.
- [2] W. E. Clark, M. Elhamdadi, X. Hou, M. Saito, T. Yeatman *Connected quandles associated with pointed abelian groups*, preprint.
- [3] M. Graña, *Indecomposable racks of order  $p^2$* , Beiträge Algebra Geom. **45** (2004), 665 - 676.
- [4] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), 917 - 923.
- [5] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge, 1991.
- [6] G. Murillo and S. Nelson, *Alexander quandles of order 16*, J. Knot Theory Ramifications **17** (2008), 273 - 278.
- [7] G. Murillo and S. Nelson, *Erratum: Alexander quandles of order 16*, J. Knot Theory Ramifications **18** (2009), 727.
- [8] S. Nelson, *Classification of finite Alexander quandles*, Topology Proc. **27** (2003), 245 - 258.
- [9] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. **8** (1907), 71 - 91.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SOUTH FLORIDA, TAMPA, FL 33620

*E-mail address:* xhou@usf.edu

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 2$				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^2}$	$[b], b \in \mathbb{Z}_{p^2}^\times$	$p^0$ if $b = 1$	1	$p^2 - p$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p}$	$p - 1$	
		$p^2$ if $b \not\equiv 1 \pmod{p}$	$(p - 2)p$	
$\mathbb{Z}_p^2$	$\begin{bmatrix} b & \\ & c \end{bmatrix}, 0 < b \leq c < p$	$p^0$ if $b = c = 1$	1	$\binom{p}{2}$
		$p^1$ if $b = 1 < c$	$p - 2$	
		$p^2$ if $b > 1$	$\binom{p-1}{2}$	
$\mathbb{Z}_p^2$	$\begin{bmatrix} b & 1 \\ & b \end{bmatrix}, b \in \mathbb{Z}_p^\times$	$p^1$ if $b = 1$	1	$p - 1$
		$p^2$ if $b \neq 1$	$p - 2$	
$\mathbb{Z}_p^2$	$\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix}, X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^2$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}(p^2 - p)$

$n = 3$				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^3}$	$[b], b \in \mathbb{Z}_{p^3}^\times$	$p^0$ if $b = 1$	1	$p^3 - p^2$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p^2}$	$p - 1$	
		$p^2$ if $b \not\equiv 1 \pmod{p^2}, b \equiv 1 \pmod{p}$	$p(p - 1)$	
		$p^3$ if $b \not\equiv 1 \pmod{p}$	$p^2(p - 2)$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p$	$\begin{bmatrix} b & \\ & c \end{bmatrix}, b \in \mathbb{Z}_{p^2}^\times, c \in \mathbb{Z}_p^\times$	$p^0$ if $b = 1, c = 1$	1	$p(p - 1)^2$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p}, c = 1$ or $b = 1, c \neq 1$	$2p - 3$	
		$p^2$ if $b \not\equiv 1 \pmod{p}, c = 1$ or $b \neq 1, b \equiv 1 \pmod{p}, c \neq 1$	$(p - 2)(2p - 1)$	
		$p^3$ if $b \not\equiv 1 \pmod{p}, c \neq 1$	$p(p - 2)^2$	

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued) $n = 3$  (continued)

$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p$	$\begin{bmatrix} b & 0 \\ 1 & b \end{bmatrix}, 0 < b < p$	$p^1$ if $b = 1$	1	$p - 1$
		$p^3$ if $b \neq 1$	$p - 2$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p$	$\begin{bmatrix} b & p \\ \gamma & b \end{bmatrix}, 0 < b < p, \gamma \in \mathbb{Z}_p$	$p^1$ if $b = 1, \gamma = 0$	1	$p(p - 1)$
		$p^2$ if $b = 1, \gamma \neq 0$	$p - 1$	
		$p^3$ if $b \neq 1$	$p(p - 2)$	
$\mathbb{Z}_p^3$	$\begin{bmatrix} b & & \\ & c & \\ & & d \end{bmatrix}, 0 < b \leq c \leq d < p$	$p^0$ if $b = c = d = 1$	1	$\binom{p+1}{3}$
		$p^1$ if $b = c = 1 < d$	$p - 2$	
		$p^2$ if $b = 1 < c$	$\binom{p-1}{2}$	
		$p^3$ if $b > 1$	$\binom{p}{3}$	
$\mathbb{Z}_p^3$	$\begin{bmatrix} b & 1 & \\ & b & \\ & & c \end{bmatrix}, b, c \in \mathbb{Z}_p^\times$	$p^1$ if $b = c = 1$	1	$(p - 1)^2$
		$p^2$ if $b = 1, c \neq 1$ or $b \neq 1, c = 1$	$2(p - 2)$	
		$p^3$ if $b \neq 1, c \neq 1$	$(p - 2)^2$	
$\mathbb{Z}_p^3$	$\begin{bmatrix} b & 1 & \\ & b & 1 \\ & & b \end{bmatrix}, b \in \mathbb{Z}_p^\times$	$p^2$ if $b = 1$	1	$p - 1$
		$p^3$ if $b \neq 1$	$p - 2$	
$\mathbb{Z}_p^3$	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 \end{bmatrix}, X^3 + b_2X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^3$	$\frac{1}{3}(p^3 - p)$	$\frac{1}{3}(p^3 - p)$
$\mathbb{Z}_p^3$	$\begin{bmatrix} 0 & 1 & \\ -b_0 & -b_1 & \\ & & c \end{bmatrix}, X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}, c \in \mathbb{Z}_p^\times$	$p^2$ if $c = 1$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}p(p - 1)^2$
		$p^3$ if $c \neq 1$	$\frac{1}{2}(p^2 - p)(p - 2)$	

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 4$				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^4}$	$[b], b \in \mathbb{Z}_{p^4}^\times$	$p^0$ if $b = 1$	1	$p^3(p-1)$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p^3}$	$p-1$	
		$p^2$ if $b \not\equiv 1 \pmod{p^3}, b \equiv 1 \pmod{p^2}$	$p(p-1)$	
		$p^3$ if $b \not\equiv 1 \pmod{p^2}, b \equiv 1 \pmod{p}$	$p^2(p-1)$	
		$p^4$ if $b \not\equiv 1 \pmod{p}$	$p^3(p-2)$	
$\mathbb{Z}_{p^3} \times \mathbb{Z}_p$	$\begin{bmatrix} b & \\ & c \end{bmatrix}, b \in \mathbb{Z}_{p^3}^\times, c \in \mathbb{Z}_p^\times$	$p^0$ if $b = 1, c = 1$	1	$p^2(p-1)^2$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p^2}, c = 1$ or $b = 1, c \neq 1$	$2p-3$	
		$p^2$ if $b \not\equiv 1 \pmod{p^2}, b \equiv 1 \pmod{p}, c = 1$ or $b \neq 1, b \equiv 1 \pmod{p^2}, c \neq 1$	$2(p-1)^2$	
		$p^3$ if $b \not\equiv 1 \pmod{p}, c = 1$ or $b \not\equiv 1 \pmod{p^2}, b \equiv 1 \pmod{p}, c \neq 1$	$p(p-2)(2p-1)$	
		$p^4$ if $b \not\equiv 1 \pmod{p}, c \neq 1$	$p^2(p-2)^2$	
$\mathbb{Z}_{p^3} \times \mathbb{Z}_p$	$\begin{bmatrix} b & 0 \\ 1 & b \end{bmatrix}, 0 < b < p^2, b \not\equiv 0 \pmod{p}$	$p^1$ if $b = 1$	1	$p(p-1)$
		$p^2$ if $b \neq 1, b \equiv 1 \pmod{p}$	$p-1$	
		$p^4$ if $b \not\equiv 1 \pmod{p}$	$p(p-2)$	
$\mathbb{Z}_{p^3} \times \mathbb{Z}_p$	$\begin{bmatrix} b & p^2 \\ \gamma & b \end{bmatrix}, 0 < b < p^2, b \not\equiv 0 \pmod{p}, \gamma \in \mathbb{Z}_p$	$p^1$ if $b = 1, \gamma = 0$	1	$p^2(p-1)$
		$p^2$ if $b \neq 1, b \equiv 1 \pmod{p}$ or $b = 1, \gamma \neq 0$	$p^2-1$	
		$p^4$ if $b \not\equiv 1 \pmod{p}$	$p^2(p-2)$	
$\mathbb{Z}_{p^2}^2$	$\begin{bmatrix} b & \\ & c \end{bmatrix}, 0 < b \leq c < p^2$	$p^0$ if $b = c = 1$	1	$(p^{\binom{p-1}{2}+1})$
		$p^1$ if $b = 1 < c, c \equiv 1 \pmod{p}$	$p-1$	
		$p^2$ if $b = 1, c \not\equiv 1 \pmod{p}$ or $b, c \neq 1, b, c \equiv 1 \pmod{p}$	$p(p-2) + \binom{p}{2}$	
		$p^3$ if $\{b, c\} = \{b_1, c_1\}, b_1 \not\equiv 1 \pmod{p}, c_1 \neq 1, c_1 \equiv 1 \pmod{p}$	$p(p-1)(p-2)$	
		$p^4$ if $b, c \not\equiv 1 \pmod{p}$	$\binom{p(p-2)+1}{2}$	
$\mathbb{Z}_{p^2}^2$	$\begin{bmatrix} b & p \\ 0 & b \end{bmatrix}, b \in \mathbb{Z}_{p^2}^\times$	$p^1$ if $b = 1$	1	$p(p-1)$
		$p^2$ if $b \neq 1, b \equiv 1 \pmod{p}$	$p-1$	
		$p^4$ if $b \not\equiv 1 \pmod{p}$	$p(p-2)$	

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 4$ (continued)				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^2}^2$	$\begin{bmatrix} b & p \\ -pb_0 & b - pb_1 \end{bmatrix}, \quad 0 < b < p, \quad X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^2$ if $b = 1$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}p(p-1)^2$
		$p^4$ if $b \neq 1$	$\frac{1}{2}(p^2 - p)(p-2)$	
$\mathbb{Z}_{p^2}^2$	$\begin{bmatrix} b + p\alpha & 1 \\ p\gamma & b \end{bmatrix}, \quad 0 < b < p, \quad \alpha, \gamma \in \mathbb{Z}_p$	$p^2$ if $b = 1, \gamma = 0$	$p$	$p^2(p-1)$
		$p^3$ if $b = 1, \gamma \neq 0$	$p(p-1)$	
		$p^4$ if $b \neq 1$	$p^2(p-2)$	
$\mathbb{Z}_{p^2}^2$	$\begin{bmatrix} p\alpha & 1 + p\beta \\ -b_0 & -b_1 \end{bmatrix}, \quad \alpha, \beta \in \mathbb{Z}_p, \quad 0 \leq b_0, b_1 < p, \quad X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^4$	$\frac{1}{2}p^2(p^2 - p)$	$\frac{1}{2}p^2(p^2 - p)$
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & & \\ & c & \\ & & d \end{bmatrix}, \quad b \in \mathbb{Z}_{p^2}^\times, \quad 0 < c \leq d < p$	$p^0$ if $b = 1, c = d = 1$	1	$\frac{1}{2}p^2(p-1)^2$
		$p^1$ if $b \neq 1, b \equiv 1 \pmod{p}, c = d = 1$ or $b = 1, c = 1 < d$	$2p - 3$	
		$p^2$ if $b \not\equiv 1 \pmod{p}, c = d = 1$ or $b \neq 1, b \equiv 1 \pmod{p}, c = 1 < d$ or $b = 1, c > 1$	$\frac{1}{2}(p-2)(5p-3)$	
		$p^3$ if $b \not\equiv 1 \pmod{p}, c = 1 < d$ or $b \neq 1, b \equiv 1 \pmod{p}, c > 1$	$\frac{1}{2}(p-2)(3p^2 - 6p + 1)$	
		$p^4$ if $b \not\equiv 1 \pmod{p}, c > 1$	$\frac{1}{2}p(p-1)(p-2)^2$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & 0 & 0 \\ 1 & b & 0 \\ 0 & 0 & c \end{bmatrix}, \quad 0 < b < p, \quad c \in \mathbb{Z}_p^\times$	$p^1$ if $b = 1, c = 1$	1	$(p-1)^2$
		$p^2$ if $b = 1, c \neq 1$	$p-2$	
		$p^3$ if $b \neq 1, c = 1$	$p-2$	
		$p^4$ if $b \neq 1, c \neq 1$	$(p-2)^2$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & p & 0 \\ 0 & b & 0 \\ \eta & 0 & b \end{bmatrix}, \quad 0 < b < p, \quad \eta \in \mathbb{Z}_p$	$p^1$ if $b = 1, \eta = 0$	1	$p(p-1)$
		$p^2$ if $b = 1, \eta \neq 0$	$p-1$	
		$p^4$ if $b \neq 1$	$p(p-2)$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & p & 0 \\ 1 & b & 0 \\ 0 & 0 & b \end{bmatrix}, \quad 0 < b < p$	$p^2$ if $b = 1$	1	$p-1$
		$p^4$ if $b \neq 1$	$p-2$	

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 4$ (continued)				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & & \\ & c & 1 \\ & & c \end{bmatrix}, b \in \mathbb{Z}_{p^2}^\times, c \in \mathbb{Z}_p^\times$	$p^1$ if $b = 1, c = 1$	1	$p(p-1)^2$
		$p^2$ if $b \neq 1, b \equiv 1 \pmod{p}, c = 1$ or $b = 1, c \neq 1$	$2p - 3$	
		$p^3$ if $b \not\equiv 1 \pmod{p}, c = 1$ or $b \neq 1, b \equiv 1 \pmod{p}, c \neq 1$	$(p-2)(2p-1)$	
		$p^4$ if $b \not\equiv 1 \pmod{p}, c \neq 1$	$p(p-2)^2$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & 0 & 0 \\ 0 & b & 1 \\ 1 & 0 & b \end{bmatrix}, 0 < b < p$	$p^2$ if $b = 1$	1	$p - 1$
		$p^4$ if $b \neq 1$	$p - 2$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & p & 0 \\ 0 & b & 1 \\ \eta & 0 & b \end{bmatrix}, 0 < b < p, \eta \in \mathbb{Z}_p$	$p^2$ if $b = 1, \eta = 0$	1	$p(p-1)$
		$p^3$ if $b = 1, \eta \neq 0$	$p - 1$	
		$p^4$ if $b \neq 1$	$p(p-2)$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & & & \\ & c & & \\ & & d & \\ & & & e \end{bmatrix}, 0 < b \leq c \leq d \leq e < p$	$p^0$ if $b = c = d = e = 1$	1	$\binom{p+2}{4}$
		$p^1$ if $b = c = d = 1 < e$	$p - 2$	
		$p^2$ if $b = c = 1 < d$	$\binom{p-1}{2}$	
		$p^3$ if $b = 1 < c$	$\binom{p}{3}$	
		$p^4$ if $b > 1$	$\binom{p+1}{4}$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & 1 & & \\ & b & & \\ & & c & \\ & & & d \end{bmatrix}, b \in \mathbb{Z}_p^\times, 0 < c \leq d < p$	$p^1$ if $b = 1, c = d = 1$	1	$\frac{1}{2}p(p-1)^2$
		$p^2$ if $b \neq 1, c = d = 1$ or $b = 1, c = 1 < d$	$2(p-2)$	
		$p^3$ if $b \neq 1, c = 1 < d$ or $b = 1, c > 1$	$\frac{1}{2}(p-2)(3p-5)$	
		$p^4$ if $b \neq 1, c > 1$	$\frac{1}{2}(p-1)(p-2)^2$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & 1 & & \\ & b & & \\ & & c & 1 \\ & & & c \end{bmatrix}, 0 < b \leq c < p$	$p^2$ if $b = c = 1$	1	$\binom{p}{2}$
		$p^3$ if $b = 1 < c$	$p - 2$	
		$p^4$ if $b > 1$	$\binom{p-1}{2}$	

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 4$ (continued)				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & 1 & & \\ & b & 1 & \\ & & b & \\ & & & c \end{bmatrix}, b, c \in \mathbb{Z}_p^\times$	$p^2$ if $b = c = 1$	1	$(p-1)^2$
		$p^3$ if $b = 1, c \neq 1$ or $b \neq 1, c = 1$	$2(p-2)$	
		$p^4$ if $b \neq 1, c \neq 1$	$(p-2)^2$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & 1 & & \\ & b & 1 & \\ & & b & 1 \\ & & & b \end{bmatrix}, b \in \mathbb{Z}_p^\times$	$p^3$ if $b = 1$	1	$p-1$
		$p^4$ if $b \neq 1$	$p-2$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} 0 & 1 & & \\ -b_0 & -b_1 & & \\ & & 0 & 1 \\ & & -c_0 & -c_1 \end{bmatrix}, \begin{matrix} X^2 + b_1X + b_0, X^2 + c_1X + c_0 \in \mathbb{Z}_p[X] \text{ irr} \\ (b_0, b_1) \leq (c_0, c_1) \text{ (*)} \end{matrix}$	$p^4$	$\binom{\frac{1}{2}(p^2-p)+1}{2}$	$\binom{\frac{1}{2}(p^2-p)+1}{2}$
$\mathbb{Z}_p^4$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ -b_0 & -b_1 & 0 & 1 \\ & & 0 & 1 \\ & & -b_0 & -b_1 \end{bmatrix}, X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^4$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}(p^2 - p)$
$\mathbb{Z}_p^4$	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 & -b_3 \end{bmatrix}, X^4 + b_3X^3 + b_2X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^4$	$\frac{1}{4}(p^4 - p^2)$	$\frac{1}{4}(p^4 - p^2)$

(\*)  $\leq$  is a total order in  $\mathbb{Z}_p^2$

TABLE 1. Nonisomorphic  $\Lambda$ -modules of order  $p^n$ ,  $n \leq 4$  (continued)

$n = 4$ (continued)				
$(M, +)$	matrix of $t$	$ (1-t)M $	number	total
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & p & & \\ \gamma & b & & \\ & & & c \end{bmatrix}, 0 < b < p, \gamma \in \mathbb{Z}_p, c \in \mathbb{Z}_p^\times, b \not\equiv c \pmod{p}$	$p^2$ if $b=1, \gamma=0, c \not\equiv 1$	$p-2$	$p(p-1)(p-2)$
		$p^3$ if $b \not\equiv 1, c=1$ or $b=1, \gamma \not\equiv 0, c \not\equiv 1$	$(p-2)(2p-1)$	
		$p^4$ if $b \not\equiv 1, c \not\equiv 1$	$p(p-2)(p-3)$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} 0 & 1 & 0 & \\ 0 & 0 & 1 & \\ -b_0 & -b_1 & -b_2 & \\ & & & c \end{bmatrix}, X^3 + b_2X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}, c \in \mathbb{Z}_p^\times$	$p^3$ if $c=1$	$\frac{1}{3}(p^3 - p)$	$\frac{1}{3}(p^3 - p)(p-1)$
		$p^4$ if $c \neq 1$	$\frac{1}{3}(p^3 - p)(p-2)$	
$\mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$	$\begin{bmatrix} b & & & \\ & 0 & 1 & \\ & -c_0 & & -c_1 \end{bmatrix}, b \in \mathbb{Z}_{p^2}^\times, X^2 + c_1X + c_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^2$ if $b=1$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}p^2(p-1)^2$
		$p^3$ if $b \neq 1, b \equiv 1 \pmod{p}$	$\frac{1}{2}(p^2 - p)(p-1)$	
		$p^4$ if $b \not\equiv 1 \pmod{p}$	$\frac{1}{2}(p^2 - p)p(p-2)$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} 0 & 1 & & \\ -b_0 & -b_1 & & \\ & & c & \\ & & & d \end{bmatrix}, X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}, 0 < c \leq d < p$	$p^2$ if $c=d=1$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{4}p^2(p-1)^2$
		$p^3$ if $c=1 < d$	$\frac{1}{2}(p^2 - p)(p-2)$	
		$p^4$ if $c > 1$	$\frac{1}{2}(p^2 - p)\binom{p-1}{2}$	
$\mathbb{Z}_p^4$	$\begin{bmatrix} b & 1 & & \\ & b & & \\ & & 0 & 1 \\ & & -c_0 & -c_1 \end{bmatrix}, b \in \mathbb{Z}_p^\times, X^2 + c_1X + c_0 \in \mathbb{Z}_p[X] \text{ irr}$	$p^3$ if $b=1$	$\frac{1}{2}(p^2 - p)$	$\frac{1}{2}p(p-1)^2$
		$p^4$ if $b \neq 1$	$\frac{1}{2}(p^2 - p)(p-2)$	